

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Jamie Frates, a Task Force Officer (“TFO”) with the Federal Bureau of Investigation (“FBI”), Kansas City, Missouri, being duly sworn, depose and state as follows:

1. I make this affidavit in support of applications under Rule 41 of the Federal Rules of Criminal Procedure for warrants to search the residence of DANIEL JAMES STREET, as described in **Attachment A1**, and the person of DANIEL JAMES STREET, as described in **Attachment A2** for the items described in **Attachment B**.

2. As a TFO, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States. At all times throughout this affidavit I use the terms “child pornography” and “child sexual abuse material (“CSAM”) merely as shorthand to refer to visual depictions of actual minors engaged in sexually explicit conduct. I use the terms “visual depiction,” “minor,” and “sexually explicit conduct” as those terms are defined in 18 U.S.C. § 2252.

3. I am currently employed as a Detective with the Kansas City, Missouri Police Department and serving as a TFO with the FBI. I have been employed with the Kansas City, Missouri Police Department since July of 2003, and am currently assigned to the FBI Child Exploitation Task Force, Kansas City, Missouri. Since February of 2022, I have been assigned to investigate computer crimes, including violations against children. I have gained knowledge in the conduct of such investigations through training in classes, and everyday work related to conducting these types of investigations. I have attended training provided by the FBI. These trainings have included instruction related to the laws against sexual abuse of minors, online applications used to entice children to produce sexually explicit material or engage in sexually explicit conduct with adults, and other subjects related to offenses committed against minor

children. I have assisted in the investigation of approximately 12 child pornography cases. During that time, I have had to view thousands of images of child pornography. I have previously applied the federal definition of child pornography used in this affidavit to a dozen search warrant applications.

4. Since this affidavit is being submitted for the limited purpose of showing that there is probable cause for the requested warrant, I have not included each and every fact known to me concerning this investigation.

PROBABLE CAUSE

5. On February 21, 2022, an online covert employee (“OCE”) in the Oklahoma City FBI Division was communicating on a social media platform with an investigative subject (not the subject of this investigation) and received a MEGA link containing over two thousand videos and images depicting child sexual abuse and child erotica material. An example of a video file in the MEGA link is entitled, “9yo Latin Girl and Lucky Man,” and shows a nude pre-pubescent female engaged in oral sex and sexual intercourse with an adult male. Another example of a video file in the MEGA link (file number 1_5086998461253943369) shows an adult male anally sodomizing a pre-pubescent male with an adult sex toy, and then anally sodomizing him with his erect penis.

6. Oklahoma City FBI requested account details from MEGA LIMITED on the owner and creator of the link, which returned information verifying the account was registered with the email blueyez_guy@yahoo.com. The registered first name of the account was “Daniel,” and the last name was “James.”

7. On April 8, 2022, a subpoena was issued to Yahoo requesting subscriber information for the blueyez_guy@yahoo.com email. On April 8, 2022, Yahoo provided subscriber information for the account, that included the first name “Dan” and the last name

“James,” and a recovery phone number of (719) 371-3130. The records also indicated the account was currently active with a registration date of January 10, 2018.

8. An open-source search on April 13, 2022, for phone number (719) 371-3130 showed the subscriber to be “Daniel Street.” Further open-source searches conducted on May 18, 2022, for (719) 371-3130 showed the number to be a T-Mobile account owned by Daniel James Street, Social Security Number XXX-XX-1070. Daniel James Street showed a birth date of August 19, 1986, based on law enforcement database records associated with said Social Security Number.

9. MEGA provided “session details” for the blueyez_guy@yahoo.com account, to include an “account creation” date of January 19, 2022, at internet protocol (IP) address 99.184.69.103.

10. On April 11, 2022, affiant determined IP address 99.184.69.103 was associated with an AT&T account. On April 11, 2022, a subpoena requesting subscriber information for the IP address was issued to AT&T. AT&T returned the requested subscriber information on May 2, 2022, which showed the service and billing address for the IP address to be 743 North Kiger Road, Independence, Missouri. The service was established in May of 2021.

11. The rental property manager for 743 North Kiger Road, Independence, Missouri stated the tenants, neither of whom were Daniel James Street, notified her on May 11, 2022, that they had moved out of the property. On the same day, affiant met the property manager, who signed a consent to search, allowing a search of the property. Affiant located a piece of mail in a small trash can inside the residence. The piece of mail was from Venmo Mastercard, addressed to Daniel Street, 743 North Kiger Road, Independence, Missouri. Missouri employment records show Street worked at the same company with one of said tenants from January through March of 2022.

12. On May 10, 2022, Daniel James Street's former employer was contacted in Gladstone, Missouri, where he worked until December 2020. The contact phone number provided to said employer by Street was (719) 371-3130, which is the same phone number associated with the creation of the MEGA link containing over two thousand images of CSAM in approximately February of 2022.

13. On May 18, 2022, Daniel James Street's current employer was contacted in Independence, Missouri. Street's current address, based on their records, is 603 North Lexington, Harrisonville, Missouri. His current phone number is different from (719) 371-3130, based on their records. A copy of Street's Colorado driver license was in their records, which showed a photo of Street.

14. On May 19, 2022, surveillance was conducted at Street's current place of employment in Independence, Missouri. At approximately 7:00 a.m., a maroon Buick Encore, driven by a female and with Daniel Street sitting in the front passenger seat, was observed driving away from Street's place of employment. At approximately 8:00 a.m., the Buick Encore was observed parked in the driveway at 603 North Lexington, Harrisonville, Missouri.

15. On June 1, 2022, a further review of the content of the MEGA link created by Daniel James Street, revealed several explicit images and videos of an individual that affiant has positively identified to be Daniel James Street. One image shows him completely naked, and a video shows him masturbating.

16. On July 15, 2022, an OCE in the Jacksonville, Florida division was connected to the internet on several occasions in an online undercover capacity from a mobile device. While using Kik, which is a free mobile cell phone application that permits users to send text messages

and other content, including videos and images, Kik user “papakock” engaged in a private message conversation with the OCE.

17. During the conversation with the OCE, “papakock” sent at least two videos of child pornography. Both videos depicted a fully nude prepubescent female child whose anus and genitalia are fully exposed to the camera, making it the focal point of the video.

18. During the conversation with OCE, “papakock” sent a MEGA link containing hundreds of video files, containing CSAM. One video file showed an adult male anally penetrating an infant with his penis.

19. On approximately July 19, 2022, law enforcement officers affiliated with the Jacksonville, Florida FBI contacted MEGA to inquire about the MEGA account that created said MEGA link. MEGA informed Jacksonville, Florida FBI that the MEGA link belonged to the account with email address blueyez_guy@yahoo.com and provided basic subscriber information associated with that account. MEGA also advised that the same account had been investigated on March 30, 2022 by an Oklahoma City, Oklahoma FBI Agent. I recognize this account information as being the same account owned by Daniel James Street as explained in this affidavit.

20. On July 20, 2022, an OCE in the San Francisco, California division was connected to the internet on several occasions in an online undercover capacity from a mobile device. While using Kik, Kik user “papakock” (with display name James Daniels) engaged in group chat message conversation with the OCE.

21. During the conversation with the OCE, “papakock” posted several video files of child pornography. One of the videos portrayed a minor prepubescent female wearing a pajama top but no bottoms kneeling on a couch reading a book. The video begins by closely showing her

anus and genitalia before zooming out. At the end of the video, she removes her top and is completely nude. Another video, this one of bestiality, shows a dog penetrating a minor female.

22. On August 16, 2022, a review of the San Francisco OCE chat was reviewed. One video posted by “papakock” showed Daniel Street’s face giving oral sex to his girlfriend, who he stated was 43 years old. It further showed a tattoo on his girlfriend’s lower back that had the name “Cody James” in the design. Another video posted by “papakock” shows an apparent live video of himself masturbating and ejaculating with a child’s car seat in the background.

23. Daniel Street’s Facebook page was located using open sources, which indicated he was in a relationship with Kimberly Davis. Kimberly Davis’ Facebook page was located from a link provided by Daniel Street’s page. On Kimberly Davis’ page, she indicates that she has children with the names “Cody and Robin.” On Davis’ account, there were photographs of her face. Using police databases, a driver’s license record was revealed for Kimberly Davis, with a date of birth of July 20, 1979, making her currently 43 years of age, with a current address of 5322 NW 70th Place, apartment 302, Kansas City, Missouri. The image with the driver’s license is the same individual pictured in the aforementioned Kimberly Davis’ Facebook photographs.

24. On August 16, 2022, surveillance was conducted on 5322 NW 70th Place, Kansas City, Missouri. A white with pink accents Jeep SUV, located parked next to Street’s vehicle (Gray Ford Fusion), bearing Missouri license plate RH5-X4V. Missouri Department of Revenue records for the license plate on the Jeep revealed that the vehicle registered to Kimberly Davis with an address of 5322 NW 70th Place, Kansas City, Missouri.

25. On August 17, 2022, at approximately 12:45 p.m., surveillance was conducted on 5322 NW 70th Place, Kansas City, Missouri. Kimberly Davis and an unknown male exited the common access door of 5322 NW 70th Place and entered the white Jeep SUV. Surveillance

followed the Jeep to a Walmart store, which was located at 8551 North Boardwalk Avenue, Kansas City, Missouri, where it parked. Kimberly Davis was observed exiting the front passenger side door of the vehicle and then walking to the front driver's side window of the Jeep. The driver rolled down the driver's side window at which time Daniel Street was observed in the driver's seat of the Jeep. A short time later, Street drove from Walmart back to 5322 NW 70th Place. Street exited the driver's door and walked up to and entered the common access door with the numbers 5322 displayed by the door.

26. It is affiant's opinion that Street is presently residing with his girlfriend Kimberly Davis at 5322 NW 70th Place, apartment #302, Kansas City, Missouri. He and his vehicle have been seen at that residence on multiple occasions. It also appears that Street is no longer residing at the Harrisonville address based on recent surveillance.

DEFINITIONS

27. The following definitions apply to this Affidavit and Attachment B:

a. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

b. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the

visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

c. “Computer,” as used herein, refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device” and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

d. “Computer hardware,” as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, “thumb,” “jump,” or “flash” drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

e. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security

software may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

f. “Hyperlink” refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

g. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

h. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

i. An “Internet Protocol address” or “IP address,” as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers (“ISPs”) control a range of IP addresses. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular

IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times. There are currently two versions of IP addresses, Internet Protocol Version 4 (“IPv4”) and Internet Protocol Version 6 (“IPv6”). Currently, IPv4 is the most widely used internet protocol for connecting devices to the Internet. IPv6 is simply an evolutionary upgrade which will ultimately replace IPv4. IPv6 was created to address the concern that the demand for IP addresses would eventually exceed the available supply. IPv6 is designed to allow the Internet to grow steadily, both in terms of the number of hosts connected and the total amount of data traffic transmitted.

j. “Minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

k. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

l. “Remote computing service,” as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

m. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

n. A “storage medium” is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, “thumb,” “jump,” or “flash” drives, CD-ROMs, and other magnetic or optical media.

o. “URL” is an abbreviation for Uniform Resource Locator and is another name for a web address. URLs are made of letters, numbers, and other symbols in a standard form. People use them on computers by clicking a pre-prepared link or typing or copying and pasting one into a web browser to make the computer fetch and show some specific resource (usually a web page) from another computer (web server) on the Internet.

p. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

q. A “Website” consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Markup Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

BACKGROUND ON COMPUTERS, CELL PHONES, AND CHILD PORNOGRAPHY

28. Computers and computer technology have revolutionized the way in which individuals interested in child pornography interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. There were definable costs involved with the production of pornographic images.

To distribute these on any scale required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings and telephone calls.

29. The development of computers has changed this. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

30. Child pornographers can now transfer photographs from a camera onto a computer-readable format with a device known as a scanner. With the advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world.

31. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

32. A smartphone, or smart phone, is a mobile phone with more advanced computing capability and connectivity than basic feature phones. Early smartphones typically combined the features of a mobile phone with those of another popular consumer device, such as a personal digital assistant (PDA), a media player, a digital camera, or a GPS navigation unit. Modern smartphones include all of those features plus the features of a touchscreen computer, including web browsing, Wi-Fi capability, and apps. Frequently, smartphones also include removable storage devices, or SD cards, where users can store data, including picture and video files. Unlike

traditional computer systems, smartphones are easily transportable and concealable, and routinely can be found on someone's person or in their vehicle.

33. Smart phone technology has expanded computer capability in recent years by allowing users to access the Internet via their phone. The smart phone user can search the Internet for specific files, check personal email accounts, log on to social networking sites, communicate with other computer users, compose and edit documents, and store and view movie and picture files.

34. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

35. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Google, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

36. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically

stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer to peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

37. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, evidence of child pornography can be found on the user's computer in most cases.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

38. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

39. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

40. In addition, there is probable cause to believe that the computer and its storage devices, the monitor, keyboard, and modem are all instrumentalities of the crime(s), within the meaning of 18 U.S.C. §§ 2251 through 2256 and should all be seized as such.

41. This application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the device was used, the purpose of its use, who used it,

and when. There is probable cause to believe that this forensic electronic evidence might be on the device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and

passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

42. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. Traditionally used forensic methods to target information specifically related to an offense, such as keyword searches for related terms, are not compatible with all types of files and applications on the device. Therefore, the examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

43. *Data outside the scope of the warrant.* Any information discovered on the device to be seized which falls outside the scope of the warrant will be returned (assuming it is legally permissible to do so) or, if copied, destroyed within a reasonably prompt amount of time after the information is identified.

SEARCH METHODOLOGY TO BE EMPLOYED

44. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

- a. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;
- b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
- c. surveying various file directories and the individual files they contain;
- d. opening files in order to determine their contents;
- e. scanning storage areas;
- f. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and/or
- g. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

MEGA LIMITED

45. Mega is a cloud storage and file hosting service maintained by Mega Limited based in Auckland, New Zealand. The service is offered through web browsers and web-based apps for Android, iPhone and Windows and can be accessed from traditional computers along with smart phones and tablets. Mega stores these files using end-to-end encryption which prevents anyone, including Mega itself, from accessing or viewing the files or folders without the encryption key.

Files or folders can then be shared with other individuals by creating a “link” (i.e., a hyperlink) to the file or folder.

46. According to Mega, Mega has a zero tolerance policy for child sexual abuse material. If any such child sexual abuse material is discovered, Mega will disable or close the account and report it to local and/or international authorities. Mega will voluntarily provide basic subscriber information data to authorities for accounts that contain child sexual abuse material. Mega can also access the content of a Mega link without a password or account recovery key, since the link contains the encryption key to decrypt the file or folder.

**CHARACTERISTICS COMMON TO INDIVIDUALS INVOLVED IN THE
DISTRIBUTION, RECEIPT, OR POSSESSION OF CHILD PORNOGRAPHY OR IN
THE CONSPIRACIES OR ATTEMPTS TO COMMIT THOSE CRIMES**

47. The majority of individuals who collect child pornography are persons who have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.

a. The majority of individuals who collect child pornography collect sexually explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. The majority of these individuals also collect child erotica, which may consist of images or text that do not rise to the level of child pornography but which nonetheless fuel their deviant sexual fantasies involving children.

b. The majority of individuals who collect child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. This contact also helps these individuals to rationalize and

validate their deviant sexual interest and associated behavior. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, P2P, e-mail, e-mail groups, bulletin boards, IRC, newsgroups, instant messaging, and other similar vehicles.


c. The majority of individuals who collect child pornography maintain books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject of sexual activities with children as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals rarely destroy these materials because of the psychological support they provide.

d. The majority of individuals who collect child pornography often collect, read, copy or maintain names, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or merely on scraps of paper.

e. The majority of individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage their collections of illicit materials. **THEY ALMOST ALWAYS MAINTAIN THEIR COLLECTIONS IN THE PRIVACY AND SECURITY OF THEIR HOMES OR OTHER SECURE LOCATION.**

CONCLUSION

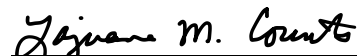
48. Based on the aforementioned factual information, your affiant respectfully submits that there is probable cause to believe that an individual, specifically DANIEL JAMES STREET, possesses child pornography in violation of 18 U.S.C. § 2252. Additionally, there is probable cause to believe that evidence of the commission of criminal offenses, namely, violations of 18 U.S.C. § 2252 may be found in DANIEL JAMES STREET'S current residence, listed in Attachment A1 , and on the person of DANIEL JAMES STREET listed in Attachment A2 to this affidavit, which is incorporated herein by reference, is contraband, the fruits of crime, or things otherwise criminally possessed, or property which is or has been used as the means of committing the foregoing offenses.



 Jamie Erates, Task Force Officer
 Federal Bureau of Investigation

Sworn and subscribed to me by telephone on this 23rd day of August, 2022.

Sworn to by telephone
 10:09 AM, Aug 23, 2022



 HONORABLE LAJUANA M. COUNTS
 United States Magistrate Judge
 Western District of Missouri

